LETTER FROM THE AUDITOR OF PUBLIC ACCOUNTS
FINANCE AND ADMINISTRATION CABINET

In Reference to the Statewide Single Audit of the Commonwealth of Kentucky

For the Year Ended June 30, 2003

CRIT LUALLEN
AUDITOR OF PUBLIC ACCOUNTS
www.kyauditor.net

105 SEA HERO ROAD, SUITE 2
FRANKFORT, KY 40601-5404
TELEPHONE (502) 573-0050
FACSIMILE (502) 573-0067

TABLE OF CONTENTS

TABLE OF CONTENTS

CRIT LUALLEN
AUDITOR OF PUBLIC ACCOUNTS

Robbie Rudolph, Secretary
Finance and Administration Cabinet

MANAGEMENT LETTER

Pursuant to KRS 43.090 (1), which states, "[i]mmediately upon completion of each audit and investigation, except those provided for in KRS 43.070, the Auditor shall prepare a report of his findings and recommendations," we are providing this letter to the Finance and Administration Cabinet to comply with KRS 43.090.

This letter presents the results of the work performed at the Finance and Administration Cabinet as part of our annual audit of the Commonwealth of Kentucky's financial statements.

In planning and performing our audit of the basic financial statements of the Commonwealth for the year ended June 30, 2003, we considered the Finance and Administration Cabinet's internal control in order to determine our auditing procedures for the purpose of expressing an opinion on the financial statements and not to provide assurance on internal control. However, we noted certain matters involving the internal control and its operation that we considered to be reportable conditions under standards established by the American Institute of Certified Public Accountants. Reportable conditions involve matters coming to our attention relating to significant deficiencies in the design or operation of internal control that, in our judgment, could adversely affect the Finance and Administration Cabinet's ability to record, process, summarize, and report financial data consistent with the assertions of management in the financial statements.

Our consideration of internal control was for the limited purpose described in the preceding paragraph and would not necessarily disclose all matters that might be reportable conditions. In addition, because of inherent limitations in internal control, errors or fraud may occur and not be detected by such controls.

As part of our audit of the Commonwealth's basic financial statements, we also performed tests of the Finance and Administration Cabinet's compliance with certain provisions of laws, regulations, contracts, and grants, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. The results of those tests disclosed no instances of noncompliance that are required to be reported under *Government Auditing Standards.*

105 SEA HERO ROAD, SUITE 2
FRANKFORT, KY 40601-5404
TELEPHONE 502.573.0050
FACSIMILE 502.573.0067
WWW.KYAUDITOR.NET

Robbie Rudolph, Secretary
Finance and Administration Cabinet

Some findings are Other Matters that we have included in this letter to communicate with management in accordance with *Government Auditing Standards*.

Included in this letter are the following:

- Acronym List
- Findings and Recommendations (Reportable Conditions, and Other Matters)
- Summary Schedule of Prior Year Audit Findings

We have issued our Statewide Single Audit of the Commonwealth of Kentucky that contains Finance and Administration Cabinet's findings, as well as those of other agencies of the Commonwealth. This report can be viewed on our website at www.kyauditor.net.

This letter is intended solely for the information and use of management and federal awarding agencies and pass-through entities and is not intended to be and should not be used by anyone other than these specified parties.

Respectfully submitted,

Crit Luallen
Auditor of Public Accounts

CRIT LUALLEN
AUDITOR OF PUBLIC ACCOUNTS

Robbie Rudolph, Secretary
Finance and Administration Cabinet

MANAGEMENT LETTER

Pursuant to KRS 43.090 (1), which states, "[i]mmediately upon completion of each audit and investigation, except those provided for in KRS 43.070, the Auditor shall prepare a report of his findings and recommendations," we are providing this letter to the Finance and Administration Cabinet to comply with KRS 43.090.

This letter presents the results of the work performed at the Finance and Administration Cabinet, as part of our annual Statewide Single Audit of the Commonwealth of Kentucky.

In planning and performing our audit over compliance with requirements applicable to major federal programs, for the year ended June 30, 2003, we considered the Finance and Administration Cabinet's internal control in order to determine our auditing procedures for the purpose of expressing an opinion on compliance with requirements applicable to each major federal program and to report on internal control over compliance in accordance with Office of Management and Budget (OMB) Circular A-133 and on the Schedule of Expenditure of Federal Awards (SEFA).

We noted certain matters involving internal control over compliance and its operation that we considered to be reportable conditions under standards established by the American Institute of Certified Public Accountants. Reportable conditions involve matters coming to our attention relating to significant deficiencies in the design or operation of internal control over compliance that, in our judgment, could adversely affect the FAC's ability to administer a major federal program in accordance with the applicable requirements of OMB Circular A-133.

As part of our audit of the Commonwealth's basic financial statements, we also performed tests of the Finance and Administration Cabinet's compliance with certain provisions of laws, regulations, contracts, and grants, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. The results of those tests disclosed no instances of noncompliance that are required to be reported under *Government Auditing Standards.*

105 SEA HERO ROAD, SUITE 2
FRANKFORT, KY 40601-5404

TELEPHONE 502.573.0050
FACSIMILE 502.573.0067
WWW.KYAUDITOR.NET

Robbie Rudolph, Secretary
Finance and Administration Cabinet

Some findings are Other Matters that we have included in this letter to communicate with management in accordance with A*uditing Standards Generally Accepted in the United States of America and Government Auditing Standards*.

Included in this letter are the following:

- Acronym List
- Findings and Recommendations (Reportable and Other Matters)
- Summary Schedule of Prior Year Audit Findings

We have issued our Statewide Single Audit of the Commonwealth of Kentucky that contains FAC's findings, as well as those of other agencies of the Commonwealth. This report can be viewed on our website at www.kyauditor.net.

This letter is intended solely for the information and use of management and federal awarding agencies and pass-through entities and is not intended to be and should not be used by anyone other than these specified parties.

Respectfully submitted,

Crit Luallen
Auditor of Public Accounts

LIST OF ABBREVIATIONS/ACRONYMS

AIL	Agency Implementation Lead
AOC	Administrative Office of the Courts
APA	Auditor of Public Accounts
ASL	Agency Security Lead
BDC	Backup Domain Controllers
CAFR	Comprehensive Annual Financial Report
CAMRA	Complete Asset Management Reporting and Accounting System
CFDA	Catalog of Federal Domestic Assistance
CFR	Code of Federal Regulations
CIM	Compaq Insight Management Web Agents
CIO	Chief Information Officer
CMIA	Cash Management Improvement Act
Commonwealth	Commonwealth of Kentucky
DBA	Database Administrators
DCA	Division of Contracting and Administration
DMPS	Department of Materials and Procurement Services
DVD	Digital Versatile Disc
FAC	Finance and Administration Cabinet
FAP	Finance and Administration Policy
FAS	Financial Analysis System
FAS.V2	Financial Analysis System Version Two
Finance	Finance and Administration Cabinet
FTP	File Transfer Protocol
FY	Fiscal Year
GASB	Governmental Accounting Standards Board
GOT	Governor's Office for Technology
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Over Secure Socket Layer
ID	Identification
INQR	Inquiry
JGTRRA	Jobs and Growth Tax Relief Reconciliation Act
KAR	Kentucky Administrative Regulation
KRS	Kentucky Revised Statute
LAN	Local Area Network
LSA	Local Security Authority
MARS	Management Administrative Reporting System
MRDB	Management Reporting Database
N/A	Not Applicable
NT	New Technology
OFM	Office of Financial Management
OMB	Office of Management and Budget
OTS	Office of Technology Service
PC	Personal Computer
PCR	Program Change Request
PD	Procurement Desktop
PDC	Primary Domain Controller
SAS	Statistical Analysis System

LIST OF ABBREVIATIONS/ACRONYMS

SDLC	System Development Life Cycle
SEFA	Schedule of Expenditures of Federal Awards
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SWCAP	Statewide Cost Allocation Plan
TSA	Treasury-State Agreement
US	United States

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 03-FAC-1: The Finance And Administration Cabinet Should Ensure Proper Classification And Categorization Of Investments In The Cash And Investment Note

The Finance and Administration Cabinet's (FAC) Comprehensive Annual Financial Reporting team prepares the Cash and Investments note (Note 5). The team uses confirmations and independent audit reports to compile summary sheets for each entity that is a part of the Commonwealth. The summary sheets for each state government entity provide cash and investments classifications and categorizations. In reviewing supporting information for each summary sheet, problems were noted in the classification and categorization of cash and investments.

Classification

In reviewing the summary sheets prepared by FAC, we noted some classification errors in fiscal years 2001 and 2002. This year, of the nine (9) summary sheets examined, we found one (1) had securities incorrectly classified by type of investment. For example, common stocks were classified as government securities for the Kentucky Teachers' Retirement System. All classification errors were corrected by FAC upon recommendation by the Auditor of Public Accounts (APA).

Although the total cash and investments reported on the Statement of Net Assets is correct, improper classification would cause the Note 5 disclosure to not agree with the classification of cash and investments reported in the Statement of Net Assets and could cause Note 5 to mislead a user as to the liquidity and asset allocation of the Commonwealth's investment portfolio.

Good internal controls dictate that investments be classified correctly according to type.

Categorization

In reviewing the summary sheets prepared by FAC, we noted some categorization errors in FY 02. This year, of the nine summary sheets examined, we found two (2) had uncategorized cash that was incorrectly reported as category 3. All categorization errors were corrected by FAC upon recommendation by the APA.

Improper categorization could cause Note 5 cash and/or investments to be overstated/understated, which could mislead the user about the credit risk for a particular investment.

According to GASB 3 Implementation Guide, *Deposits with Financial Institutions, Investments (including Repurchase Agreements), and Reverse Repurchase Agreements*, Question 4, there are three (3) credit risk categories used to report cash and investments information depending on "who the securities custodian is and how the securities custodian holds the security."

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 03-FAC-1: The Finance And Administration Cabinet Should Ensure Proper Classification And Categorization Of Investments In The Cash And Investment Note (Continued)

Categorization (Continued)

The categories required for reporting are as follows:

1. The custodian is the government's agent and is not the counterparty or the counterparty financial institution's trust department. The custodian holds the securities in the government's name.

2. The custodian is the counterparty financial institution's trust department or the counterparty's agent and the custodian holds the securities in the government's name.

3. The custodian is the counterparty, regardless of whether it holds the securities in government's name.

Or the custodian is the counterparty financial institution's trust department or the counterparty's agent and the custodian does not hold the securities in the government's name.

If the investment is not insured or registered or if collateral or investment is not in the possession of the government, then the investment is required to be categorized in one of the above categories.

Recommendation

Classification

We recommend FAC establish a procedure that would provide greater assurance that investments agree by classification to independent audit reports and other supporting documentation.

Categorization

We recommend consistent and proper categorization of investments be done for each state government entity for Note 5, as required by GASB 3.

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 03-FAC-1: The Finance And Administration Cabinet Should Ensure Proper Classification And Categorization Of Investments In The Cash And Investment Note (Continued)

Management's Response and Corrective Action Plan

Procedures are in place to assure proper classification and categorization of investments, yet at times mistakes are made. The Financial Reporting Team strives for consistency and accuracy in the presentation of Note 5 as required by GASB 3. We will add a procedure to have an individual review, at a minimum, the major agencies to ensure proper classification and categorization of investments.

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 03-FAC-2: The Finance And Administration Cabinet Should Strive To Ensure That All State Agencies Conduct Accurate And Timely Fixed Assets Inventory Counts

FAC's Division of Statewide Accounting Services requires an annual physical inventory of fixed assets by all state agencies. FAC provides a Physical Inventory Procedures Manual for conducting the annual physical inventory. This manual provides details of how to conduct the fixed assets inventory count.

We observed fixed assets inventory counts at several agencies during our FY 03 Fixed Assets audit. Two (2) agencies, Administrative Office of the Courts (AOC) and Department of Parks, had serious deficiencies with fixed assets inventory count procedures. Our audit findings and agency responses are outlined below:

Administrative Office of the Courts

We observed inventory counts at the AOC Fayette County, Franklin County, and Jefferson County locations. We noted that AOC personnel conducting the inventory counts did not follow the policies and procedures outlined in FAC's Physical Inventory Procedures Manual.

Recommendation

We recommend that AOC conduct an annual inventory count of fixed assets following the policies and procedures outlined in the FAC's Physical Inventory Procedures Manual. This would include using the 5003 Fixed Assets report to record the results of the inventory observation; searching for and adding unrecorded fixed assets; verifying and correcting the tag number, description, location, serial number, agency, organization and asset type for each asset; and making every effort to locate missing items. This would also include having adequately instructed individuals conducting the inventory counts.

Management's Response and Corrective Action Plan

The AOC Department of Facilities' Property Accountability Branch, through the course of its statewide inventory in compliance with audit rules and procedures, provided State Auditor personnel weekly notices of locations and dates the 5003 inventory would be conducted. State Auditor personnel were present for portions of this process in Fayette, Franklin, and Jefferson counties.

During a June 19, 2003, meeting, State Auditor personnel presented their findings to AOC personnel after all but seven (7) items had been accounted for statewide. These items included an item (presumed to be a printer) purchased in 1981, a video recorder system purchased in 1984, and information technology components, which likely have been relocated to other counties or declared surplus over the past decade.

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 03-FAC-2: The Finance And Administration Cabinet Should Strive To Ensure That All State Agencies Conduct Accurate And Timely Fixed Assets Inventory Counts (Continued)

Administrative Office of the Courts (Continued)

Management's Response and Corrective Action Plan (Continued)

AOC anticipates locating most of these items upon completion of its statewide property accountability audit.

State Auditor personnel noted that items were not found in Jefferson County. Most items were located on the initial inspection. Further, some items were located from the Court of Justice property accountability system via telephone. Additional research by AOC personnel enabled the inventory to be successfully completed on a subsequent visit, with the exception of three of the seven items previously discussed. State Auditor personnel were not present during this visit.

State Auditor personnel discussed a problem with 5003 copy "ownership." They stated that State Auditor 5003 "copies" (identical to AOC copies) were used for inventory purposes by AOC personnel in Jefferson County. This statement was true. Auditor personnel in Louisville expressed a desire to split into two groups for the sake of time. AOC obliged and performed as requested. Each group used a set of 5003 documents, one group with AOC's copy, the other with the State Auditor's copy. State Auditor personnel arrived on-site in Frankfort without 5003 documents and relied on AOC copies of the document.

AOC continues to extend an invitation to State Auditor personnel to accompany and observe its accountability processes throughout the Commonwealth and welcomes an inspection of its inventory system.

AOC concurs with the goals stated in the report's "Recommendation" narrative and will strive to achieve those goals. For the next inventory of items with a purchase price of $5,000 and above, the Court of Justice will use bar-code reading devices for greater accuracy and accountability. AOC is conducting a statewide, 100-percent inventory that is capturing and verifying, tag numbers, descriptions, locations, agency, organization, and asset type for Court of Justice property. AOC is recording data not required via the FAC report such as serial numbers, manufacturers, room numbers, floor numbers, and photographs of some items. It is anticipated that this inventory will take one year to complete.

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 03-FAC-2: The Finance and Administration Cabinet Should Strive To Ensure That All State Agencies Conduct Accurate And Timely Fixed Assets Inventory Counts (Continued)

Administrative Office of the Courts (Continued)

Auditor's Reply

The auditor's role in the fixed assets inventory count process is to observe agency personnel performing the count and observe whether agency personnel follow proper procedures for the count. The auditor is not an extension of the agency and does not arrive at the inventory count with the intention to help find and count the inventory. Auditors are not required to bring any documents to the inventory count; rather they are required to obtain a copy of the agency's completed inventory record upon leaving. When auditors observe agency personnel not following proper procedures, this creates an audit finding for that agency.

In addition, any inventory items "found" after the auditor has left the site cannot be verified and therefore cannot be considered found for audit purposes.

We acknowledge that the agency is attempting to implement better procedures for the next fixed assets inventory count and encourage them to continue this effort.

Department of Parks

We observed fixed assets inventory counts at 17 state parks. At ten of the parks, we noted a variety of control weaknesses, including that personnel conducting the inventory counts did not follow the policies and procedures outlined in FAC's Physical Inventory Procedures Manual.

We also conducted a test to confirm that historical treasures were correctly entered and tracked in the MARS fixed assets inventory system. We tested 66 items and noted that six (6) items were not entered in the MARS fixed assets inventory system and six (6) additional items were incorrectly valued.

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 03-FAC-2: The Finance And Administration Cabinet Should Strive To Ensure That All State Agencies Conduct Accurate And Timely Fixed Assets Inventory Counts (Continued)

Department of Parks (Continued)

Recommendation

We recommend that Department of Parks conduct an annual inventory count of fixed assets following the policies and procedures outlined in FAC's Physical Inventory Procedures Manual. This would include using the 5003 Fixed Assets report to record the results of the inventory observation; searching for and adding unrecorded fixed assets; verifying and correcting the tag number, description, location, serial number, agency, organization and asset type for each asset; and making every effort to locate missing items. This would also include having adequately instructed individuals conducting the inventory counts.

We further recommend that Department of Parks enter all historical treasures into the MARS fixed assets inventory using the correct values as recorded in the collection of historical treasure "books" on file at Department of Parks.

Management's Response and Corrective Action Plan

The Kentucky Department of Parks intends to fully cooperate and follow the procedures that are outlined in the Finance and Administration's Physical Inventory Procedures Manual.

The Fixed Asset section in the Parks Department is in the process of updating and verifying the fixed assets of Parks. The department recently completed a follow up inventory and correction documents have been processed to record the results of the physical inventory. The property officer for Parks has led this effort.

Parks management will make sure all staff responsible for conducting the physical count in the future is aware of the procedures outlined in the Finance Procedures Manual. We will make every effort to locate and record the Parks fixed assets accurately in MARS.

The Historical Treasures and Artifact inventory is being verified. Currently two employees, Property Officer and the Assistant Director, are comparing the historical treasure "books" with MARS. They are correcting any discrepancies that are located. Parks is also in the process of having accredited appraisals of our Historic Treasures and Artifacts, as funds become available. Our intention is to have our Historic Treasures appraised over the next few years.

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 03-FAC-2: The Finance And Administration Cabinet Should Strive To Ensure That All State Agencies Conduct Accurate And Timely Fixed Assets Inventory Counts (Continued)

Department of Parks (Continued)

Management's Response and Corrective Action Plan (Continued)

We will update our records at the completion of each independent appraisal and notify the Department of Insurance of the value of the items appraised.

We are in the process of conducting physical inventory of our Historic Treasures and Artifacts. After completion the records will again be updated in MARS.

We appreciate the findings and view this an opportunity to correct the deficiency cited.

Finance and Administration Cabinet

Recommendation

We recommend that FAC strive to have all agencies follow policies and procedures outlined in the Physical Inventory Procedures Manual and to provide technical assistance whenever necessary to ensure that inventory counts are conducted correctly and accurately reflect the fixed assets of the Commonwealth. We further recommend that FAC conduct training and closely monitor those agencies that consistently have inventory problems from year to year.

Management's Response and Corrective Action Plan

FAC has provided The Inventory Observation Procedures to the agencies through the Closing Schedule. Additionally FAC is offering classes on Inventory Observation Procedures.

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 03-FAC-3: The Finance And Administration Cabinet Should Ensure All User Accounts On Its Agency Machines Are Necessary

During the security vulnerability assessment testing for machines controlled by the FAC, we found several instances where it appears unnecessary user accounts were established on machines or for applications.

To examine the information provided by NetBIOS, we limited our review to 36 machines including the Primary Domain Controller (PDC), Backup Domain Controllers (BDC), SQL servers, and NT servers. NetBIOS account information was received from 16 machines, including the PDC and nine (9) BDCs, within the FAC domain. We examined the NetBIOS information from one (1) of the BDCs to search for disabled or unused accounts. There were 1,809 accounts on the BDC. The BDC contained 84 disabled accounts, or 4.6 percent, and 13 locked out accounts, or 0.7 percent. While reviewing other FAC machines, we found the guest account on five (5) other machines that had been disabled, but not removed.

To determine possible unnecessary accounts, the auditor used the criteria that the account was over the 30-day maximum password age established by the Finance and Administration Cabinet (Finance) policy and had never logged onto the system. The BDC had 87 accounts, or 4.8 percent, that met this criterion. Further, while examining other Finance machines, we found an additional machine that had four (4) user accounts that had not been logged onto within 30 days of being established.

The auditor attempted a remote logon to known applications using various combinations of default logon passwords. A review of all machines controlled by Finance revealed 80 machines with port 21 open and 61 machines with port 23 open.

We were able to create a File Transfer Protocol (FTP) session through port 21 on 34 machines, or 42.5 percent, using the anonymous or guest logins. In the prior year audit, 32 of these machines were also noted with port 21 related weaknesses. In addition, Telnet sessions could be established with no login or through the anonymous or guest default logins on 35 machines, or 57.4 percent, through port 23. In the prior year audit, 34 of these same machines were noted with port 23 related weaknesses.

Intruders often use inactive accounts to break into a network. If an account has not been used for a reasonable period of time, the account should be disabled until it is needed. This minimizes the possibility that an unauthorized user will access the account. An account should be deleted if it is not going to be reinstated. Further, default administrator, guest, and anonymous accounts in operating system and applications are some of the first accounts that an intruder will attempt to use. Therefore, they should be assigned strong passwords or, if possible, renamed or removed immediately after installation.

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 03-FAC-3: The Finance And Administration Cabinet Should Ensure All User Accounts On Its Agency Machines Are Necessary (Continued)

Recommendation

We recommend that Finance review accounts on all their machines to determine which accounts have had no password change within the last 30 days. These accounts should be evaluated to determine if they are still valid accounts required for a business-related purpose. If not, the accounts should be disabled or deleted as appropriate. Further, Finance should ensure that all machines with FTP or Telnet services running on them restrict access to default, anonymous, or guest logons.

Management's Response and Corrective Action Plan

The Finance Cabinet has carefully reviewed the accounts in the domain and removed several hundred obsolete accounts. Several accounts will remain disabled due to the fact they are used for Mailbox accounts for conference rooms or special email accounts that are used as a RESPOND TO account only. The accounts are not directly accessed via email, but are managed through another email account. It is impossible by design to remove the guest account from the Microsoft Windows Operating System.

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 03-FAC-4: The Finance And Administration Cabinet Should Secure Listings Of User Names And Associated User IDs For Power Users Of The Management Administrative And Reporting System

FAC has provided a list of state employee power users for Seagate Reporting software by agency name on a public Management Administrative Reporting System (MARS) website. This listing is accessible to any Internet user through the use of common web browsers and includes sensitive User IDs for the noted users.

Seagate Reporting power users listed on this site have the authority to create, design, schedule and view reports of financial and other sensitive information stored on the MARS data servers. User ID information and associated user names at this level by agency could also be used to identify naming conventions and determine IDs of other high profile system users. Provision of this level of security information is not consistent with FAC formal policy and procedures concerning security governing MARS data.

Further, the MARS Seagate password does not expire and users of this reporting system are not required to change passwords after a period of time. Internet users currently can obtain information about MARS Seagate Reporting users such as their name, location, and their User ID. Once a potentially unauthorized intruder knows a User ID, a password cracking software can be initiated for guessing as often as necessary to obtain unofficial access to the Commonwealth's information. In many cases the type of information that might be provided would include sensitive information that should be properly secured. The security of the Commonwealth's financial information is ultimately the responsibility of FAC.

Sensitive personal and financial data maintained by the Commonwealth should be properly secured. These measures should include securing IDs and passwords of users capable of accessing this type of information. Consistent application of established security policy and procedures provides continuity for implementation and sets the tone of management concern for strong system security.

Recommendation

We recommend that FAC remove the noted sensitive Seagate Reporting power user information from the general public website. If FAC sees the need to list power users for informational purposes we suggest they either find a more secure solution for providing that information or limit the information provided to name and cabinet only; the User ID should not be listed. Access to Seagate Reporting user information should be treated as confidential information, and security over that information should be maintained in a manner similar to that applied to user information for other MARS related applications.

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 03-FAC-4: The Finance And Administration Cabinet Should Secure Listings Of User Names And Associated User IDs For Power Users Of The Management Administrative And Reporting System (MARS) (Continued)

Management's Response and Corrective Action Plan

The report on the Internet has already been changed by the Finance and Administration Cabinet and the user ID is no longer listed. Only the agency/cabinet and the name of the report designer (power user) are listed.

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 03-FAC-5: The Finance And Administration Cabinet Should Develop And Implement Formal Policy And Procedures To Govern Security Of The Management Administrative And Reporting System Interface Files

FAC did not develop and implement formal policy and procedures identifying management and user responsibilities concerning security governing MARS Interface Files.

It is ultimately the responsibility of FAC to ensure that access to MARS interface files is reasonable. Our review for the FY 03 revealed that 11 users had update access to checkwriter files as well as authorization to request these files be processed through FAC.

During the prior FY, we noted that FAC had forwarded a letter addressing the procedures for requesting users access, to each agency security lead (ASL). Additionally, FAC had performed procedures to alert agency security leads on the importance of segregating the duties of updating interface files and authorizing these files to be processed. They verified each agency's security lead's awareness of user access to interface files by providing them with a list of datasets, all users within their agency that have access to them, and the type of access provided. Each ASL was required to take responsibility for such access by returning a signed Advantage Financial Security Agreement. This agreement states that the security surrounding the datasets, for which employees have access, provide sufficient internal controls to ensure that the actions initiated through the datasets are in accordance with the objectives of the agency. However, at the time of fieldwork FAC had not performed procedures to review the reasonableness of access to MARS interface files. We feel that incorporating such procedures into a formalized security policy will ensure procedures governing access to MARS interface files are performed on a regular basis.

Consistent application of formalized security policy and procedures provides continuity for implementation and sets the tone of management concern for strong system security. Formal policies provide a security framework used to educate management and users of their security responsibilities. To help ensure strong security and the integrity of checkwriter files, it is necessary to develop and implement a formal policy identifying management and user responsibilities concerning MARS interface files. Further, the level of system access granted to users should be restricted to only areas necessary for an employee to perform assigned job duties. Allowing users the ability to update checkwriter files and authorize their processing increases the likelihood of unauthorized processing of checkwriter data, and may compromise the integrity of data processed through MARS.

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 03-FAC-5: The Finance And Administration Cabinet Should Develop And Implement Formal Policy And Procedures To Govern Security Of The Management Administrative And Reporting System (MARS) Interface Files (Continued)

Recommendation

We recommend that FAC develop and implement a formal policy to govern the security surrounding MARS interface files. This effort should include standardizing procedures to be implemented on a regular basis. We further recommend these procedures include steps to provide for a higher level of confidence in proper segregation of duties concerning update and processing of checkwriter files.

Management's Response and Corrective Action Plan

The Finance and Administration Cabinet will develop and implement a policy to govern the security on checkwriter files. Included in the policy will be steps that will be taken to ensure segregation of duties concerning the update and the processing (E-mail request) of checkwriter files.

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 03-FAC-6: The Finance And Administration Cabinet Should Develop And Apply Formal System Development Life Cycle Procedures For The Commonwealth's Cash And Investments Statistical Analysis System Programs

The Office of Financial Management (OFM) did not develop and implement adequate formal System Development Life Cycle (SDLC) policies and procedures governing controls for program development and modifications. In addition to the lack of policies and procedures for program modification controls noted during the prior two audits, the Statistical Analysis System (SAS) system manual was not completed and formalized during FY 03. In May 2002, the programs processed to generate reports for OFM and to create Journal Voucher text files for transfer to MARS were re-written in SAS language. Subsequent to implementing the programs, a manual documenting SAS system programs was being created but remained in draft form at the time of fieldwork for FY 02. The time period between converting the system programs to SAS and the current year's review was sufficient to ensure the SAS manual was completed. However, the manual remained in incomplete and in draft form throughout FY 03. Items missing from the system manual are described below. Therefore, our comment concerning the lack of policies and procedures governing program modification controls has expanded to include the lack of system documentation as well as additional system development life cycle issues identified during current year testing.

The auditor noted 592 program modifications during FY 03. Prior to the development of the SAS programs, the OFM programmer was provided access to the previous application programs, and was verbally provided the objectives the SAS programs were to accomplish. Formal program specifications were not provided. The number and significance of the modifications made during FY 03 implies that the objectives and specifications of the programs developed may not have been clearly presented to the programmer prior to or during the initial program development. Therefore, it is necessary to comment on the lack of formal and complete program specifications provided by management prior to development or major modification of the SAS programs. Specific objectives and specifications can be provided within the currently used program change request (PCR) forms or as separate attachments to the change request forms.

The SAS system manual was not updated to include several programs that were implemented during the fiscal year and does not provide a program processing flow diagram, production procedures, or contain a complete or accurate overview for a majority of the production programs.

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 03-FAC-6: The Finance And Administration Cabinet Should Develop And Apply Formal System Development Life Cycle Procedures For The Commonwealth's Cash And Investments Statistical Analysis System Programs (Continued)

Further, OFM created and implemented the use of a production library that was intended to control OFM programmer access to production SAS programs. However, procedures and controls were not established to ensure the intended function of that library. The program modification process, as was noted during the prior year's review, allows the OFM sole programmer to test and submit the SAS programs from the programmer's personal drive, then merely request a copy of those programs be placed into the production library for audit trail purposes. However, in one (1) case we identified a file maintained within the production library was not the correct version generated during the actual production run. A separate audit comment will report that inadequate segregation of duties exist allowing the OFM programmer access rights.

Finally, the agency did not formally adopt or consistently apply policies and procedures to control program modifications. Prior to implementing the new SAS programs, OFM designed and implemented procedures involving a program change request PCR form to document the need for program modifications, description of modifications, testing of modifications, and authorization to implement modifications. However, these procedures were not formalized into policy and our testing revealed 219 of 592, or 37 percent of the program modifications were not supported by a PCR. The PCRs that were examined did not provide adequate documentation of the need for the modification, the description of modifications made, and had no signatures authorizing the implementation of the modification.

Without formalized SDLC procedures, management increases the risk of developing and implementing insecure, ineffective, or inaccurate systems and the risk of unauthorized changes being placed into the production environment that have an adverse affect on system processing results. SDLC procedures require adequate program specifications be provided to a programmer prior to program development to mitigate processing errors and the need for numerous program modifications. Sufficient procedures dictate that complete and accurate system documentation be developed and maintained for all critical systems, as this information is vital to ensuring longevity of the system. Further, SDLC procedures must be consistently applied and include adequate procedures to segregate the live production environment from development and testing environments.

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 03-FAC-6: The Finance And Administration Cabinet Should Develop And Apply Formal System Development Life Cycle Procedures For The Commonwealth's Cash And Investments Statistical Analysis System Programs (Continued)

Recommendation

We recommend that OFM develop, implement and consistently apply complete formal SDLC control procedures including providing adequate program specifications and understanding of program objectives, proper completion of system documentation, control and maintenance of test and production libraries including adequate control over the migration of program changes to production, and authorization and approval of program changes. Specifically, documented SDLC policies implemented should incorporate:

- The SAS system manual should be completed and updated appropriately to include a complete and accurate overview of all programs used in production. This overview should include flowcharts or diagrams and a description of the programs function.

- Detailed program specifications should be provided to the programmer prior to development or significant modification of SAS programs. These specifications should be retained for audit trail purposes.

- The policies should specifically state which personnel are authorized to provide approvals for each stage of the program change request. Once proper approval has been obtained to implement the changes, then the programmer should sign off that the requested changes were made.

- Proper authorization for program modifications should be obtained and documented prior to those changes being made, the necessity for the change should be explicitly stated, documentation as to the changes made should be descriptive, and testing of the modification should be evident. This information should be included upon or attached to the program change requests.

- Testing facilities should be maintained separate from the production environment.

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 03-FAC-6: The Finance And Administration Cabinet Should Develop And Apply Formal System Development Life Cycle Procedures For The Commonwealth's Cash And Investments Statistical Analysis System Programs (Continued)

Recommendation (Continued)

- A PCR should be on file for any modification where a blanket request is not acceptable. A blanket request will be accepted for modifications considered to be minor recurring maintenance. Recurring maintenance could include entering necessary parameters such as cycle number, fiscal year, date, number of days in the month, and file name changes where the file name contains a date or month that corresponds to the date/month being processed. A blanket request would also be acceptable for changes when there is a change in the referenced directory that will increase the security of production programs and data files.

- All versions of the SAS programs and data files used for or generated by daily and monthly processing should be retained for historical purposes for an established period of time.

Management's Response and Corrective Action Plan

The SAS system manual is in the process of being completed and will submitted in draft form to the APA by January 15, 2004.

The program has been in production long enough that the development-phase has past. There should not be any significant modifications going forward. If significant changes are made, proper documentation will be in-place before the modification goes into production.

A PCR has been developed and is in use. It is the goal of OFM to have a program change request for any change in the program. Discussions have taken place within OFM to ensure that all staff members understand the importance of full documentation and approval before any modifications are placed in production. We think that FY04 the APA will find we are in compliance.

Testing facilities are now maintained separately from the production environment. Programming duties and the administering of production programs have now been separated. Efforts are ongoing to ensure proper segregation of duties.

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 03-FAC-6: The Finance And Administration Cabinet Should Develop And Apply Formal System Development Life Cycle Procedures For The Commonwealth's Cash And Investments Statistical Analysis System Programs (Continued)

Management's Response and Corrective Action Plan

OFM has established a library that retains all current and former production programs. OFM's programmer does not have access to these programs nor to MARS or CAMRA. OFM's programmer can no longer run production programs.

The Office of Financial Management agrees in a large part with the findings of the Auditor of Public Accounts. OFM continues to strive to ensure that all programming is accurate and the Commonwealth's assets are properly protected.

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 03-FAC-7: The Office Of Financial Management Should Improve Segregation Of Duty Controls

As noted in the previous audit, OFM did not employ proper segregation of duties between programmer, operator, and librarian functions. During the fiscal year FY 02, SAS programs were implemented to replace a number of EXCEL and ACCESS applications that accounted for and reported the Commonwealth's cash and investments for OFM. At this time, the OFM programmer employed to develop and maintain SAS programs was provided access to SAS production programs and data. Since the prior year's review OFM has created a SAS production library, designated a librarian to move production programs to the library, and automated the compilation of daily MARS files as recommended in the audit comment from the previous year. However, OFM did not properly use the SAS production library created and the programmer continues to have full access to production programs and data. Further, the current year's review revealed the programmer has access to additional applications and data critical to the processing of the Commonwealth's cash and investments. We identified the following control weaknesses:

- The SAS program code that processes cash and investment financial data monthly requires the programmer to manually enter critical accounting data directly into the program. The data consists of calculated amounts such as payoff balances, adjustment amounts for each investment pool, and security lending balances for the month. All values are assigned to macro variables used throughout the program. Available supporting documentation was not sufficient to substantiate the data entered. The documentation did not provide evidence of review, detail of the calculations where applicable, and in most instances supervisory authorization.

- Programs in development or testing are not controlled or segregated from the programs that are in production. Movement of production files and programs to the production library is at the discretion of the programmer. Files and programs are not currently moved into the production library until after the SAS production run is complete.

- Test and production programs and data files are maintained on the programmer's personal network drive. Hence the programmer has full access to the directory housing this information. Currently, production output is written and saved to the programmer's personal drive(s).

- The programmer also functions as the operator for these programs, submitting the production programs for processing on a routine basis.

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 03-FAC-7: The Office Of Financial Management Should Improve Segregation Of Duty Controls (Continued)

- The programmer manually modified the production version of the Journal Voucher text file prior to its upload to MARS for the July 2002 distribution. The documentation provided in support for this modification did not reflect evidence of supervisory review or authorization.

- The programmer has full access to the Complete Asset Management, Reporting, and Accounting System (CAMRA) that stores the critical investments data used by SAS to create the journal voucher to distribute monthly investment earnings.

- The programmer has enter, correct, and delete access and first level of approval to major documents and tables within MARS. The SAS generated journal voucher that distributes investment earnings monthly is recorded in MARS.

Employing strong segregation of duty controls decreases the opportunity for unauthorized modification to files and programs, and the likelihood of errors or losses occurring from incorrect use of data, programs, and other resources. Programmer duties should not include the input of accounting data, discretionary migration of programs into production libraries, or performing operator procedures such as executing production programs. Programmers should be restricted from the production environment and their activities should be conducted solely on "test" data. Programmers should not have access to the production environment. This control should be designed to ensure an independent and objective testing environment without jeopardizing the integrity of production data.

Computer operators should not have direct access to program source code. The function of this control is to ensure that the computer operator does not intentionally or unintentionally introduce unauthorized or malicious source code into production. Smaller organizations that cannot easily segregate programmer duties from computer operator duties should implement compensatory controls to supervise programmer activities to ensure only properly tested and authorized programs are migrated into production.

Recommendation

We recommend that OFM take the necessary actions to discontinue the processes that allow programmer access to production programs and data. OFM should also eliminate procedures requiring the programmer to input accounting information into production programs. OFM should take the following actions to employ proper segregation of duty controls:

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 03-FAC-7: The Office Of Financial Management Should Improve Segregation Of Duty Controls (Continued)

Recommendation (Continued)

- Request modification of the program code that performs month-end processing to eliminate the need for the programmer to manually enter accounting data. The programs should be developed to call in text or other input files generated by accounting personnel.

- Ensure SAS programs are properly tested prior to migrating them to production to ensure the integrity of the programs.

- Ensure the production library is used to house only the proper versions of production programs and data, and that programs affecting production are run only from that library. Discontinue the process of allowing the programmer to run programs affecting production from his personal library. This may require implementing an application or modifying the programs to include security that will force the program to write to the production library without the operator or programmer having edit, update, or delete access to the library.

- Designate a computer operator other than the programmer to execute the production programs. Also, implement access controls to ensure the operator can only read and execute programs in the production environment.

- Ensure controls are implemented to maintain an audit trail for identifying applicable production programs used during the year for the period suitable for audit purposes.

- Eliminate the programmer's full access to CAMRA. If a situation occurs requiring the programmer to access CAMRA, the programmer's access should be set to 'read' or 'reporting' at the maximum as appropriate.

- Eliminate the programmer's enter, correct, delete access and first level of approval authority to MARS documents and tables.

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 03-FAC-7: The Office Of Financial Management Should Improve Segregation Of Duty Controls (Continued)

Recommendation (Continued)

Circumstances of an emergency nature requiring the programmer to have update access privileges should be granted only for the time period required to address the situation and must be documented and closely monitored at the appropriate supervisory level. For these circumstances a log should be created that specifically documents the individual accessing the production library by user ID, time of entry, specific programs and data accessed and purpose and the time access was deleted. All activity should be subject to supervisory control and system log entries should be substantiated by a formal request for the access granted.

Management's Response and Corrective Action Plan

Action has been taken to eliminate the programmer's access to production programs and data. The program operator is separate from the programmer. Further, action is being taken that will eliminate procedures requiring the programmer to input accounting information into production programs and requiring the programmer manually enter accounting data.

All new programs and modifications to programs must have a program change form filled out. One of the sections on this form requires the internal auditor or some other staff member to test the modification before it is placed in production.

All daily production programs are housed in the Library and data is written to the History folder when programs are run daily by the operator. Monthly production programs will be handled the same way when testing is complete.

Any program changes made to the programs in the library will be accompanied by documentation identifying the changes. Only production programs are in the production library. Test programs are run on the programmer's PC.

The programmer's access to CAMRA has been set to "Reporting".

The programmer's access to MARS documents and tables has been changed to INQR (Inquiry) security group which allows 'view – only' access.

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 03-FAC-8: The Finance And Administration Cabinet Should Track Federal Expenditures For The Jobs And Growth Tax Relief Reconciliation Act In MARS

In FY 03, Finance received $68,720,606 for the Jobs and Growth Tax Relief Reconciliation Act (JGTRRA). Through JGTRRA, the U. S. Treasury provided funds to states to be used for general government purposes under Catalog of Federal Domestic Assistance (CFDA) 21.999. In reviewing Finance's Schedule of Expenditures of Federal Awards for the Act, we discovered Finance had failed to adequately track the expenditure of these funds as suggested by OMB Circular A-133 or the Act. Although the funds were deposited into the general fund, and we could confirm the receipt of the funds, there were no procedures in place to track how these funds were spent. The Act placed limits on how the funds were to be used, and without some type of tracking procedure the APA has no way of determining if allowable costs and/or allowable activities compliance requirements are appropriately met.

We are aware that Finance has received another $68,720,606 in FY 04, which was also deposited into the general fund. Failing to properly track the funds received in FY 03, raises concerns that there are possible problems with tracking the proper use of the funds received in FY 04.

When federal funds are not individually and specifically identified, the federal fund information presented on the Schedule of Expenditures of Federal Awards cannot be reconciled to MARS. Moreover, without proper tracking of federal expenditures, we are unable to determine if allowable costs and/or allowable activities compliance requirements are appropriately met.

OMB Circular A-133 requires that we determine if federal grant funds are used for allowable costs under the requirements of federal program. The Act specifies that the funds be used for essential government needs, and specifically not for new programs.

Good internal controls dictate that receipts should be accounted for using a specific identifier to allow all related expenditures to be matched to their corresponding receipts.

Recommendation

We recommend Finance account for this federal grant in the same manner they account for their other federal grants. We recommend these funds be appropriated for a certain government need, and assigned a specific identifier in MARS.

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 03-FAC-8: The Finance And Administration Cabinet Should Track Federal Expenditures For The Jobs And Growth Tax Relief Reconciliation Act In MARS (Continued)

Management's Response and Corrective Action Plan

We agree that depositing the Jobs and Growth Tax Relief Reconciliation Act (JGTRRA) funds in the General Fund makes it difficult to track expenditures to a specific program. We were, to the best of our judgment, in compliance with the guidelines provided by the US Department of Treasury. In our application for funding we certified that the JGTRAA funds would be used to "provide essential government services for types of expenditures permitted in the most recently approved budget". We did not track expenditures to a specific program in fiscal year 2003. We plan to implement your recommendation in fiscal year 2004 and allot the JGTRAA funds to a specific program and track expenditures at the program level.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 03-FAC-9: The Division Of Contracting And Administration Should Ensure Proper Segregation Of Duties For The Transaction Process

During the Capital Projects audit, the Division of Contracting and Administration (DCA) did not employ proper segregation of duties in the transaction process. We noted the following weakness in DCA's internal controls:

- The Accountant processing the invoices for the vendor is also the same accountant picking the check up from Treasury for the vendor.

Recommendation

Duties within the DCA should be separated so that one staff member does not perform processing from the beginning to the end of a process. Assigning different staff the responsibilities of authorizing transactions, recording transactions, and maintaining custody of assets is recommended to reduce the opportunities to allow any individual to be in a position to both perpetrate and conceal errors and irregularities or fraud in the normal course of his or her duties.

Management's Response and Corrective Action Plan

While we fully agree that the segregation of duties is critical to proper oversight and control of irregularities or fraud, we wish to state that the three duties listed are indeed divided, and no staff member performs the processing from beginning to end for any activity.

The capital construction invoice process is initiated by the contractor itself and is then reviewed and routed through the Architect/Engineer consultant, the project manager within the Division of Engineering and the Associate Director of Engineering prior to being submitted to the Division of Contracting and Administration to initiate the payment document.

Once received in DCA, one accountant enters the information into Procurement Desktop and applies the first level of approval, all payment transactions require at least two separate approvals to release. No individual is to have sufficient approval authority to apply all levels of approval.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 03-FAC-10: The Finance And Administration Cabinet Should Ensure That All Open Ports On Agency Machines Have A Business-Related Purpose

During the security vulnerability assessment testing for machines controlled by Finance, we found several Finance machines with ports open that may not have a specific business-related purpose. Due to the large number of issues, we grouped the findings below by port number and application.

We tested machines based on the potential for misuse of port access. We originally tested 36 Finance machines, then expanded testing to all Finance controlled machines to examine ports 80, 443, and 8000.

Port 80 – Hypertext Transfer Protocol (HTTP)
Port 80 was open on 35 machines that would not display the website. Twenty-five of these machines had been reported during the prior year. When no default page or restricted logon is required, normally this means that no application/web service is running at the port. Additionally, configuration information for printers or print servers was provided by 27 websites, 21 of these machines were reported during the prior year. This situation provides too much access to information for an unauthorized or anonymous user.

Port 443 – Hypertext Transfer Protocol over Secure Socket Layer (HTTPS)
Eight machines were found with port 443 open but would not display a website. Two of these machines had been reported during the prior year. When no default page or restricted logon is required, normally this means that no application/web service is running at the port.

Port 6667 – Internet Relay Chat
Three machines in the Finance domain were discovered with port 6667 open. Two of these machines had been reported during the prior year. This port can be used for several serious exploitations such as Denial of Service attacks, Trojan horse attacks, and downloading of illegal files. This port could be useful to a hacker and should only be used for a necessary business-related application.

Port 8000 – HTTP
Twenty-three machines owned by Finance were discovered that had port 8000 open. Twenty-two of these machines do not display the website and do not appear to have an application/web service running on them. Fifteen of these machines were reported during the prior year. The remaining machine revealed configuration information for printers for the second year. This situation provides too much access to information for an unauthorized user.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 03-FAC-10: The Finance And Administration Cabinet Should Ensure That All Open Ports On Agency Machines Have A Business-Related Purpose (Continued)

Other Ports

Three machines had ports open that do not appear to specifically relate to known business applications. One of these machines was reported during the prior year. Finance should review all open ports on machines to ensure that all have a valid business-related purpose**.**

Even though there were several machines that still had issues noted during FY 03, there has been a marked improvement in the overall number of machines with open ports for which the auditor questioned necessity.

For security purposes, detailed information concerning the specific machines or user accounts that contributed to these findings is being intentionally omitted from this comment. However, these issues were thoroughly documented and communicated to the appropriate agency personnel.

The existence of open ports is an invitation for intruders to enter your system. To minimize the risk of unauthorized access to a machine, only necessary, business-related ports should be open and all applications residing at these ports should be secured to the extent possible.

Recommendation

We recommend that Finance review all open ports on the machines discussed in this comment. If there is not a specific business-related purpose requiring a port to be open, then that port should be closed. Further, we recommend that Finance periodically review open ports on all machines owned by the agency to ensure necessity.

Management's Response and Corrective Action Plan

The Finance Cabinet is working with the GOT Firewall Team to close unnecessary access to the cabinet computer systems through a rules set that only allows specific access to the Network.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 03-FAC-11: The Finance And Administration Cabinet Should Develop Formal Procedures For System Assurance Efforts Concerning The Financial Analysis System

As noted in the previous two audits, there are no formal procedures in place for assuring the completeness or reliability of Financial Analysis System (FAS) data. FAS is a client/server reporting system that is accessed via the Internet and permits system users to analyze MARS financial data with minimal effort and expertise.

The primary source of data for this system is from the Management Reporting Database (MRDB), a component of MARS. Therefore, the Office of Technology Services (OTS) makes the assumption that the data is accurate. OTS is dependent on system users to notify the division when system errors or inaccurate data occur that should then be investigated. Often the nature of the discrepancy is not readily determined.

The FAS data is completely rebuilt each night, and a nightly cycle report is generated the following morning for review. This nightly cycle report lists the file name, file size and date of file creation. This report is manually examined only to determine that information appears reasonable. If for some reason the data does not appear complete, since OTS performs a complete rebuild each night of FAS, the next nightly cycle is expected to correct any problems. No other formal procedures are performed to assure FAS data and/or system totals are accurately downloaded for reporting purposes.

Ultimately, OTS is responsible for the support of the application and should ensure the accuracy of data. When discrepancies are noted, OTS personnel should determine the reason and best method of correcting the discrepancy. Ideally, once problems have been corrected, comparison reports should be reproduced to ensure that the problem has been corrected and that there are no further problems. There are currently no written procedures in place concerning the use of management reports to assure FAS data accuracy.

Formalized procedures and standards should be implemented for the daily FAS system assurance procedures, and should include report comparisons to MRDB. Formalized procedures should also include descriptions of the OTS employee's processes and the steps taken to resolve errors that are noted within these system assurance efforts. Further, reconciliations should be performed daily to ensure that totals agree with reports from MRDB. Formalized system assurance procedures provide continuity for procedure implementation and illustrate management's concern for strong data integrity within the system.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 03-FAC-11: The Finance and Administration Cabinet Should Develop Formal Procedures For System Assurance Efforts Concerning The Financial Analysis System (Continued)

Recommendation

We recommend that OTS develop detailed written procedures documenting the processes to be followed for the creation and review of the daily and monthly system assurance reports between the FAS and the MRDB, and for the correction of errors discovered through review of these reports. Further, these procedures should be distributed to all employees that are involved with the FAS system assurance task.

Management's Response and Corrective Action Plan

FAS is a reporting tool that obtains data from existing systems, it does not manipulate the actual figures to display on the reports. Therefore a method of system assurance would be redundant against the other systems.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 03-FAC-12: The Finance And Administration Cabinet Should Continue To Work In Conjunction With The Governor's Office For Technology To Implement Logging And Audit Features Within Procurement Desktop

As was noted in the previous three audits, the Procurement Desktop (PD) system lacks sufficient audit logging and security features, although numerous improvements have been implemented.

We noted that most weaknesses are currently being addressed and applicable security measures are in the process of planning and testing. However, though the FAC and the GOT have made considerable progress regarding PD weaknesses noted in the prior year, our review revealed that some weaknesses remain that have not been sufficiently addressed.

PD database changes are captured in an archive file that is currently kept for only one day due to space constraints and system performance. While FAC and GOT are working on potential options to archive longer, this process has not been completed. Also, access security feature enhancements for the PD system still have not been completed with regard to password expiration, consecutive password usage, and user ID lockout based on number of unsuccessful attempts for all users.

In addition, DBA's review the PD logs on a weekly basis while the SAS Director reviews them on a periodic basis. These reviews, however, are only for high-level database privilege activity and failed access attempts. Finally, it was noted that the logging system captures unsuccessful login attempts but not successful login attempts.

Transaction logging and auditing helps to ensure that only authorized access has taken place and that changes to the system are in accordance with the established security policy. Implementation of adequate intrusion detection and incident handling procedures by the data owner is essential to ensure a secure system. Management's position on the importance of system security should be noted by implementation of a thorough security policy.

Recommendation

FAC and GOT should continue to look at options for backing up and maintaining the archive log longer than one day.

FAC and GOT should ensure the new PD version currently being developed provides for the implementation of security parameters to control such things as password length, forced password changes, password history control, and unsuccessful access lockouts. Once that capability exists, FAC should further ensure those security parameters are implemented for PD user accounts that comply with the overall agency security policy for similar systems.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 03-FAC-12: The Finance And Administration Cabinet Should Continue To Work In Conjunction With The Governor's Office For Technology To Implement Logging And Audit Features Within Procurement Desktop (Continued)

Recommendation (Continued)

The PD logging procedures should be modified so that the audit database will contain successful logins as well as unsuccessful login attempts. This is to ensure repeated attempts from an intruder are exposed as well as actual illegal access. While some techniques allow review for potential intruders just with unsuccessful attempts recorded, there still would be no record of actual intrusion unless the successful attempt was logged.

The current log review schedule should be continued, at a minimum, but the review should entail looking at activity for all access level user IDs instead of just the high-level user IDs. The review should include scans for unauthorized access, account sharing, and system compromises or changes. Further, these reviews and the results should be documented for audit trail purposes.

Management's Response and Corrective Action Plan

We are currently pulling the daily logs and as I understand converting them to text and writing them to DVDs. The CIO's office delivers these recorded logs for storage on a weekly basis. We don't quite have the full year for 2003, but we are on a regular schedule.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 03-FAC-13: The Finance And Administration Cabinet Should Consistently Apply Established Program Modification Control Procedures For The Financial Analysis System

As noted in the previous two audits, the FAC does not have formal procedures in place to ensure the authorization of program modifications to the FAS. During the audit period, Finance did not maintain a log or monitor requests made for FAS program changes. All program modifications were made without formal documentation by the system developer.

Unlike other information systems, FAC does not rely on GOT to complete program modifications requested for FAS. Staff in the Office of Technology Services makes all program changes. These same employees are responsible for testing and placing FAS programs into production.

Ideally, program change requests should be documented and procedures should be in place to track the progress of requests. Program modification procedures should include system-testing efforts to ensure program modifications meet requirements. Testing facilities assure that any problems are identified and re-tested before they are placed into the production environment.

There should also be adequate documentation of user acceptance and authorization prior to placing modified programs into production. Additionally, there should be adequate segregation of duties between programmer and librarian functions. Programmers should not have ready access to production source code.

Recommendation

We recommend that FAC develop and distribute specific polices and procedures for program changes to FAS. OTS should ensure personnel are aware of and trained on the proper procedures for requesting, authorizing, monitoring, and moving into production any changes for FAS programs. Documentation of FAS program change requests, request status, and evidence of proper authorization for changes should be maintained as an audit trail.

Management's Response and Corrective Action Plan

FAC has implemented a program modification control system that includes logging of all changes to the FAS programs.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 03-FAC-14: The Finance And Administration Cabinet Should Improve Logical Security Measures Over The Financial Analysis System

FAC facilitates security access authority to the FAS through OTS. As noted in the previous two audits, OTS has not adequately established proper logical security measures for this reporting system.

Originally OTS administered the security for FAS access centrally. Now, FAS security administrators are established by OTS based on information provided through the Agency Implementation Leads (AILs) or their designee. Ideally, these security administrators would issue user IDs and passwords in an effort to control and monitor logical access. It should be noted that FAS does contain some data that is highly sensitive such as personnel data including personnel profile information like salaries and leave balances. The issues are summarized below to specifically identify security weaknesses noted within the FAS system:

FAS system does not maintain an audit feature to track ID assignments and/or user profile changes. Formal documentation did not exist on a consistent basis to support the FAS access provided to users.

Our review revealed that due to recent decentralization of FAS access administration throughout the various state agencies, 60 users have security administrator level access to update user profiles. There are currently approximately 869 FAS users. This appears to be an excessive number of employees with the ability to update user security profiles. It would be more cost efficient to control FAS access centrally.

Formal policies and procedures have not been developed and distributed to security administrators concerning FAS access security controls. Security Administrators may not fully understand their responsibilities to obtain and retain well-documented access authorization forms or email, which would support access granted and/or the access removed.

The FAS profile update capability does not limit the FAS security administrators from providing users more access than needed to perform the work for their functional area within their agency. Therefore, a FAS security administrator could issue user privileges to all agency data, when a valid user request may not require that level of access.

Each user password is readily visible in clear text by all security administrators on the security maintenance screen. This includes the passwords for other security administrators' accounts.

FAS does not force an initial password change for new users nor does the system require password changes on a frequent basis.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 03-FAC-14: The Finance And Administration Cabinet Should Improve Logical Security Measures Over The Financial Analysis System (Continued)

Training has been provided to the various FAS security administrators, but adequate training was not provided to agency supervisors responsible for requesting access for their employees. This lack of training may cause supervisors to be unaware of the consequences of profile changes they might request or authorize.

System security should be administered in such a way as to ensure proper segregation of duties, and access to FAC data should be granted on an as needed basis. Formal procedures should be established for system access controls to ensure security is not compromised. Formal documentation should be maintained to support authorization for the access actually granted FAS users. Centralized management of logical security efforts is generally viewed as a more efficient means of security administration, and will likely be more cost effective. Users with the capability to add or change user access should be limited to a few key personnel. Passwords should not be visible in clear text to users or system administrators. Supervisors and managers requesting changes to user security profiles should be properly trained.

Recommendation

We recommend FAC take the following steps to improve the logical security administration function for FAS:

OTS should establish polices and procedures for improving the logical security effort by FAS security administrators. Formal procedures should be implemented requiring submission and maintenance of documentation for FAS access requests and authorizations.

FAC should consider reinstating centralized access control responsibility for FAS within OTS.

System audit features should be activated to record system ID assignments and/or user changes.

User passwords should be shadowed, suppressed, or encrypted on the security maintenance screen to prevent unauthorized FAS access. Applicable system password files should also be encrypted.

Adequate training should be provided to supervisors and managers responsible for requesting system access to ensure they understand the consequences of profile changes requested.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 03-FAC-14: The Finance And Administration Cabinet Should Improve Logical Security Measures Over The Financial Analysis System (Continued)

Management's Response and Corrective Action Plan

A new system is in development to replace the Financial Analysis System; this new system uses common programming standards and security templates based on the commonwealth's data storage system MRDB.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 03-FAC-15: The Finance And Administration Cabinet Should Develop And Implement Formal Written Policies And Procedures Concerning Security Of The Financial Analysis System

As noted in the previous two audits, the FAC did not develop and implement formal written security policies and procedures identifying management and user responsibilities concerning security of the FAS. We recognize that FAC is currently in transition with changes being made to the infrastructure and management of FAS. However, these formal policies had not been developed as of the date of our follow-up with this comment.

FAS is a client/server reporting system that is accessed via the Internet and permits system users to analyze Management Administrative Reporting System financial data with minimal effort and expertise. There are approximately 869 current users of FAS and no formal policies have been developed concerning procedures for ensuring proper access to this reporting system. A draft policy has been prepared for use by the Customer Resource Center and has served as the primary reference for recent training of FAS Security Administrators at the agency level. If an individual requests access to FAS, they are directed to their respective FAS Security Administrator. Therefore, FAC should not only develop and implement policies concerning its central level oversight for FAS security but also disseminate policies to be followed by agency level FAS Security Administrators.

Failure to adequately document and communicate security policies could lead to a lack of understanding by management and users resulting in a failure to comply with security policy. Non-compliance with security policies may also lead to unauthorized data or program modification, destruction of assets, and interruption of services. Further, lack of documented disciplinary action procedures may allow for inconsistent treatment of security violators.

For security to be effectively implemented and maintained, detailed written policies and procedures must be developed. These procedures provide the security framework used to educate management and users of their security responsibilities. Further, formalized security policies provide continuity for policy implementation and illustrate management's concern for strong computer system and data resource security.

Recommendation

We recommend FAC develop and implement security policies and procedures that will help ensure the security of access to the FAS. This effort should include policies to be disseminated out to the FAS Security Administrators at the agency level.

Management's Response and Corrective Action Plan

A new system is in development to replace the Financial Analysis System; this new system is being developed and will be implemented with proper written policy and procedures.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 03-FAC-16: The Finance And Administration Cabinet Should Ensure That Security Information Leakage For Agency Devices Is Minimized

The FAC should restrict critical information divulged by its network machines. During our testing of the Finance local area network (LAN) security for FY 03, we discovered several instances where machines within the LAN provided information to anonymous users that could potentially divulge information that would assist in an unauthorized system attack.

The auditor ran vulnerability assessment tools twice during FY 03 on 36 machines within the Finance domain to determine if they would return information on Local Security Authority (LSA), Password Policies, Valid User, Group, or Share Lists. Both runs of the tools revealed the same results, as shown in the table below.

Type of Information	Number of Machines Returning Information	Percentage of 36 Machines Examined
LSA	26	72.2%
Password Policies	16	44.4%
Valid User List	16	44.4%
Valid Group List	16	44.4%
Valid Share List	16	44.4%

We found six (6) machines under Finance control that had port 2301 open. We were able to log onto the Compaq Insight Manager application on one of these machines with the default administrator user ID and password. This access provides too much information to a potentially unauthorized individual.

Finally, we were able to gain access through port 80 to an automated listing of heating, cooling and lighting related failure events within specific state facilities. This access was provided through a default anonymous logon. Again, this access provides too much information to a potentially unauthorized individual.

For security purposes, detailed information concerning the specific machines or user accounts that contributed to these findings is being intentionally omitted from this comment. However, these issues were thoroughly documented and communicated to the appropriate agency personnel.

An agency's domain information accessible world wide through inquiry tools or default logons should be kept at a minimum. Agencies should ensure that information such as machine location, accounts associated with the machine, data residing on the machine, and the machine's role is not accessible to the public. To accomplish this, an agency can configure machines to not respond to certain types of inquiries, can use naming conventions that obscure the purpose of machines, can provide no comments on machine activity, and can restrict access to default logons for applications.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 03-FAC-16: The Finance And Administration Cabinet Should Ensure That Security Information Leakage For Agency Devices Is Minimized (Continued)

Recommendation

We recommend that Finance restrict the information provided by its LAN machines to anonymous users. First, limitations should be placed on the type of response machines provide to system inquiries. Second, the default logons for the CIM application should be changed. Third, the security surrounding the website in question should be altered to ensure that only authorized persons are allowed access.

Management's Response and Corrective Action Plan

CIM is being removed from all Servers. We are limited on the ability to restrict further NETBIOS information from local machines due to the need to communicate with GOT mail servers. Restricting anonymous access to the domain controllers to the fullest extent prevents the Cabinet from using the GOT mail services and would require Finance to maintain it's own mail server.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 03-FAC-17: The Finance And Administration Cabinet Should Change System Defaults To Guard Against Unauthorized System Access

During the security vulnerability assessment testing for machines controlled by the FAC, we found four machines, or 11.1 percent of the 36 machines examined, that had the Simple Network Management Protocol (SNMP) service available and would allow an anonymous user to logon with the community name "public." The "public" community name is the default public account for this service. The use of the "public" community name allows too much information to be provided to any anonymous user.

Through our testing, the system provided information about listening ports, open sessions, active user accounts, and shares that exist. In comparison to the prior year audit, these machines were not included in previous findings for FY 02.

For security purposes, detailed information concerning the specific machines or user accounts that contributed to these findings is being intentionally omitted from this comment. However, these issues were thoroughly documented and communicated to the appropriate agency personnel.

Information provided by the SNMP service concerning a machine's functions could be useful to an intruder in developing an attack. Worldwide access via the Internet through the use of default logons should not be allowed.

Recommendation

We recommend that Finance either disconnect the SNMP service or change the "public" community name to a more sophisticated name on all machines. Further, any new machines should be checked for any established SNMP service to ensure the "public" community name has been changed.

Management's Response and Corrective Action Plan

The existence of the SNMP was due to the Compaq Insight Management tools being installed on the servers in question. This software was removed to correct this issue.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 03-FAC-18: The Finance And Administration Cabinet Should Consistently Apply Its Account Password Policy On All Domain Machines

During the security vulnerability assessment testing for machines controlled by the FAC, the auditor received account related information from 16 machines within the Finance domain. Twelve of these machines were also noted as providing this type of information in the prior year audit. This information was compared to agency password policy criteria. During FY 03, there has been a marked improvement in the overall number of machines with password policy settings that did not comply with the agency's policy.

The results of this comparison are illustrated in the table below.

Security Measure	Standard	Number of Machines Not in Compliance With Policy	Percentage of 16 Machines Not in Compliance with Policy
Maximum Age	30 days	4 – 42 days	25.0%
Minimum Age	Immediate – None	None	N/A
Minimum Length	6 characters	4 – None	25.0%
Lockout Threshold	5 attempts	4 – None	25.0%
Lockout Duration	"Forever" 71,582,788 minutes (approximately 136.2 years)	4 – 30 minutes	25.0%
Lockout Reset	1,440 minutes	4 – 30 minutes	25.0%

The backup domain controller (BDC) did have properly established password policies. We obtained NetBIOS information from that machine and examined the information to determine if accounts adhered to the established policy. There were 1,809 user accounts on the BDC. We found 38 accounts, or 2.1 percent, that had logged onto the system at least once that did not comply with the Finance Policy to change an account password at least every 30 days.

An additional machine was noted that had two user accounts and the administrator account that had been logged onto the system at least once but the passwords have not been changed in the last 30 days.

For security purposes, detailed information concerning the specific machines or user accounts that contributed to these findings is being intentionally omitted from this comment. However, these issues were thoroughly documented and communicated to the appropriate agency personnel.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 03-FAC-18: The Finance And Administration Cabinet Should Consistently Apply Its Account Password Policy On All Domain Machines (Continued)

Passwords are a significant feature to guard against unauthorized system access. The failure to follow adequate policy standards when establishing a system password could ultimately compromise the entire network. The purpose of a password policy is to establish a standard to create strong passwords, to protect those passwords, and to ensure passwords are changed within a specified time period. To assist in the security of a network, it is necessary for a strong policy to be developed and consistently implemented on all machines throughout the network.

Recommendation

We recommend that Finance review the password settings established on all Finance machines to ensure that the password policy is being consistently applied.

Management's Response and Corrective Action Plan

The Finance and Administration Cabinet current domain password policy is as follows:

Maximum Age:	*30 day*
Minimum Age:	*Immediate - None*
Minimum Length:	*8 characters (instead of the recommended 6 characters)*
Lockout Threshold:	*5 attempts*
Lockout Duration:	*Forever*
Lockout Reset:	*1440 Minutes*

Other machines audited are either member servers and/or Workstations with the local account policies being quoted in the audit. Local accounts are not used in this agency, Except for the local administrator account, which is reset via remote tools on a regular basis.

Actions to be taken:
Set local account policies to match domain policies as much as possible or higher.

FEDERAL AWARD FINDINGS AND QUESTIONED COSTS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 03-FAC-19: The Finance And Administration Cabinet Should Track Federal Expenditures For The Jobs And Growth Tax Relief Reconciliation Act In MARS

State Agency: Finance and Administration Cabinet
Federal Program: CFDA #21.999 Jobs And Growth Tax Relief Reconciliation Act
Federal Agency: U.S. Department of Treasury
Pass-Through Entity: Not Applicable
Compliance Area: Allowable Costs/Activities Allowed
Amount of Questioned Costs: None

This finding is a reportable condition for internal controls over financial reporting and for internal control over compliance. The entire finding is under Financial Statement Findings as 03-FAC-8.

FEDERAL AWARD FINDINGS AND QUESTIONED COSTS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 03-FAC-20: The Finance And Administration Cabinet Should Review All Eligible Cash Management Improvement Act (CMIA) Transactions Requiring Interest Calculations To Ensure That The Annual Report Is Complete And Accurate

After reviewing the Cash Management Improvement Act (CMIA) Annual Report for FY 03 and its underlying development procedures, we have concluded that the report is neither complete nor accurate. Errors discovered were caused by the FAC personnel using the incorrect threshold for state interest liability calculations on refunds and the lack of a prior year federal interest liability adjustment that had been reported to Finance originally in FY 01.

During the review of the state interest liability calculation for refunds from the federal government, we discovered that Finance was using the incorrect threshold amount. Both the CMIA regulations and the Treasury-State Agreement for FY 03 allow that the state will not incur an interest liability on refunds in refund transactions under $50,000. However, during the development of the state interest liability on refunds, Finance personnel used a threshold of $10,000. This oversight in threshold amount change caused a state interest liability to be erroneously computed on a refund transaction of $44,335.34 for CFDA #93.778. This error in state interest liability determination resulted in an overstatement of $110 in interest being paid to the federal government.

Further, an instance of an overstatement of federal interest liability, which was originally reported to Finance in FY 01, was not corrected for the second year. The original comment was issued during FY 01 after an examination of the federal interest liability determined that three projects associated with CFDA #20.205 were incorrectly established in MARS. These projects should have been associated with CFDA #20.219, which is not CMIA reportable. The documentation provided by Finance indicated 12 transactions existed in which a federal interest liability was accrued for these projects. Therefore, the $996 that was paid to the Commonwealth for FY 01 associated with these transactions should have been refunded to the federal government during one of the past two fiscal years. Although, Finance stated during FY 02 that this adjustment would be included in the FY 03 Annual Report, the correction was not made.

Ultimately, the accuracy of the CMIA Annual Report is the responsibility of Finance. To ensure that the Annual Report is correct, those responsible for the development of the Annual Report should review all reporting requirements to ensure that any changes in procedures are followed in the current year. Further, a review of recommended prior year adjustments should be made to ensure that all adjustments are included in the Annual Report.

FEDERAL AWARD FINDINGS AND QUESTIONED COSTS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 03-FAC-20: The Finance and Administration Cabinet Should Review All Eligible Cash Management Improvement Act (CMIA) Transactions Requiring Interest Calculations To Ensure That The Annual Report Is Complete And Accurate (Continued)

Recommendation

We recommend that Finance make the following corrections on the FY 04 Annual Report:

- A prior year state interest liability adjustment for CFDA 93.778 of $110.
- A prior year federal interest liability adjustment for CFDA 20.205 of $996.

Further, during the development of the FY 04 Annual Report, Finance should ensure that the correct threshold amount is used for state interest liability for refunds.

Management's Response and Corrective Action Plan

Documentation has been placed in the FY2004 CMIA workpaper folder to ensure that prior year adjustments will be made for the corrections noted for CFDA 93.778 and CFDA 20.205.

The FY 2004 Treasury-State Agreement will be reviewed prior to beginning the CMIA Annual Report process to ensure correct threshold amounts are used for refund and interest liability calculations.

FEDERAL AWARD FINDINGS AND QUESTIONED COSTS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 03-FAC-21: The Finance And Administration Cabinet Should Consistently Monitor Cash Management Improvement Act Projects To Ensure Proper Eligibility Designation

Although the FAC established procedures to ensure projects were accurately designated within the MARS in compliance with the CMIA, these procedures were not followed consistently to ensure the current CMIA Treasury-State Agreement (TSA) supported projects were designated as eligible. Specifically, the procedures were not designed to capture all CMIA eligible projects regardless of their current system designation.

The current method for determining CMIA reportable projects is to review the annual TSA for listed eligible CFDA grants. All projects associated with the listed CFDA numbers should have the CMIA Eligible toggle button (CMIA flag) switched to "Yes" within the Agency Project Table.

Our review of the established FAC procedures for creating the annual CMIA report revealed that the CMIA flag is a criterion within the development of the CMIA eligible projects database, which is later used for calculating state and federal interest liabilities. Because of the use of the CMIA flag, the established procedures would not properly ensure all CMIA flags for CMIA eligible project were appropriately set. The underlying System Query Language (SQL) queries used to develop the database only extract those projects where the CMIA flag is set to "Y". In the case of projects that would be CMIA eligible based on their associated CFDA number but had an incorrectly set CMIA flag of "N", these projects would not be identified as errors. Our review of projects associated with CMIA eligible CFDA numbers that were also federally funded, revealed 6,558 unique projects. Of these there were 60 projects, or 0.91 percent, that were found to have the CMIA flag set to "N". If the procedures for developing the CMIA eligible projects database had been properly established, these projects would have been noted as errors and corrections could have been made.

Further, as our review revealed, the established procedures do not appear to be consistently applied. In the case of those projects being set with a CMIA flag of "Y", it does not appear that FAC is properly reviewing these projects for CMIA eligibility. By reproducing the CMIA eligible project database as described by FAC, the auditors found 6,583 records that met the criteria. Of these records, there were 85 records, or 1.29 percent, that when the auditor reviewed their associated CFDA numbers were found to not be CMIA eligible according to the TSA. If the procedures as set forth by FAC for the review of the CMIA eligible projects database were functioning as described, these projects would have been noted as errors and corrections would have been made.

FEDERAL AWARD FINDINGS AND QUESTIONED COSTS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 03-FAC-21: The Finance And Administration Cabinet Should Consistently Monitor Cash Management Improvement Act Projects To Ensure Proper Eligibility Designation (Continued)

There has been discussion in prior years as to whether the CMIA flag can be relied upon for reporting of CMIA eligibility. Per recommendations in past years, the FAC has decided to use this indicator for their reporting purposes. However, this indicator cannot be used effectively unless there is absolute confidence in its integrity. FAC is ultimately responsible for the completeness and accuracy of the information within MARS. To ensure information is available and correct for reporting annually to the U.S. Treasury under the requirements of the CMIA, Finance must follow established guidelines to maintain adequate records within MARS.

Recommendation

To ensure the accuracy of the CMIA Annual Report, we recommend the following changes be made in the procedures for the development of the CMIA eligible projects database:

1. The criterion within the SQL to limit the population of the database to those records that have a CMIA flag value of "Y" must be removed. This change will provide a listing of all federally funded projects under review.

2. A separate database should be developed containing all projects that are associated with CMIA eligible CFDA numbers per the applicable TSA. These projects should be reviewed to ensure that all records have the CMIA flag set to "Y". Any records with a CMIA flag of "N" should be corrected.

3. The records not extracted into the CMIA eligible database should be reviewed to determine if the CMIA flag is set to "N". Any records where the CMIA flag is "Y" should be corrected.

Management's Response and Corrective Action Plan

We agree with your findings and will improve the process next year. Our goal will be to resolve the timing issues associated with retrieving the correct project information.

FEDERAL AWARD FINDINGS AND QUESTIONED COSTS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 03-FAC-22: The Finance And Administration Cabinet Should Adjust The Statewide Cost Allocation Plan

State Agency: Finance and Administration Cabinet
Federal Program: All CFDAs
Federal Agency: All Federal Grantors
Pass-Through Entity: Not Applicable
Compliance Area: Allowable Costs/Cost Principles
Amount of Questioned Costs: None

During the audit of Statewide Cost Allocation Plan (SWCAP), it was noted that prior year adjustments to the plan had not yet been made.

During the audit of the FY 02 SWCAP (based on 2000 actual expenditures), a recommended adjustment was made for Facilities Security, because billings to agencies in the amount of $2,086,914 from Fees from the Public were not deducted from expenses on Schedule C27. This error caused an under bill to be shown on Exhibit B of the FY 02 Plan when it should have been an over bill.

During the audit of the FY 01 SWCAP (based on 1999 expenditures) for Deferred Comp, general fees from the public were included in revenue in the 2000 Plan but not the 2001 Plan. There was confusion as to whether or not these fees should be included. After clarification, it was determined these fees should have been included in the FY 01 plan revenue. It was stated that this would be corrected by an adjustment in the amount of $4,325,463.

Improper reporting on the cost allocation plan may affect the amount of federal funds that the Commonwealth is entitled to receive.

> OMB Circular A-87 guidelines state:
>
> > Cost Allocation Plans provide the documentation to identify, accumulate and allocate, or develop billing rates based on the allowable costs of services provided by a governmental unit or centralized basis to its departments and agencies. These central service costs may be allocated or billed to users. Allocated central services costs (referred to as Section I costs) are allocated to benefiting operating departments or agencies based on some reasonable basis. Billed central service costs (referred to as Section II costs) are billed to benefiting departments, agencies and/or programs on an individual fee-for-service or similar basis.

Also, per FAC's instructions for preparing of the SWCAP, "If the audit produces any errors, they must be included as an adjustment in the next plan that is prepared."

FEDERAL AWARD FINDINGS AND QUESTIONED COSTS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 03-FAC-22: The Finance And Administration Cabinet Should Adjust The Statewide Cost Allocation Plan (Continued)

Recommendation

We recommend FAC adhere to its instructions and correct the current plan by making adjustments to Section II costs for Facilities Securities in the amount of $2,086,914 and Section I costs for Deferred Comp in the amount of $4,325,463.

Management's Response and Corrective Action Plan

Audit findings will be addressed and corrected in the current year Statewide Cost Allocation Plan.

FEDERAL AWARD FINDINGS AND QUESTIONED COSTS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 03-FAC-23: The Finance And Administration Cabinet Should Ensure Agencies Are Aware Of Contract Invoicing Procedures And Contract Modification Requirements

State Agency: Finance and Administration Cabinet
Federal Program: All CFDAs
Federal Agency: All Federal Grantors
Pass-Through Entity: Not Applicable
Compliance Area: Procurement
Amount of Questioned Costs: None

During our testing of procurement procedures, we noted a contract in which the dollar limit was exceeded. The invoice for this contract had a line added without a reference to the contract. Therefore, MARS did not detect that the contract was exceeded. The contract was not modified to allow additional expenditures.

When preparing invoices for payments on contracts in PD, agencies are not required to reference the corresponding contracts. However, agencies may be required to modify the contract in PD for any changes to the contract agreement. If invoices are not consistently referenced, and contracts are not modified as required, MARS cannot detect if the contract amount is exceeded. MARS checks contract expenditures to ensure that the contract amount is not exceeded.

Agency personnel may not be aware that lines on a contract's invoice should reference the contract, and modifications should be made, accordingly, if necessary.

Section 2 of 200 KAR 5:311 Contract modifications states: "All changes to contracts for the purchase of commodities, supplies, equipment and construction services shall be effected by a modification to the contract."

Also, good internal controls dictate a contract's invoice should reference the contract number to enable MARS to detect if contract amounts are being exceeded.

Recommendation

We recommend Finance communicate to agencies that all invoices related to contracts should reference the respective contracts, and contracts should be modified accordingly, if necessary.

FEDERAL AWARD FINDINGS AND QUESTIONED COSTS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 03-FAC-23: The Finance and Administration Cabinet Should Ensure Agencies Are Aware Of Contract Invoicing Procedures And Contract Modification Requirements (Continued)

Management's Response and Corrective Action Plan

DMPS has reviewed the report and offers the following. The comment that payments are not required to reference the contract is not correct. According to FAP 111-45-00, all payments against contracts that have been entered in the state procurement system and that encumber funds in the accounting system shall be paid in the procurement system on a document that references the contract and liquidates the encumbrance. We have drafted an article for the next MARS and Beyond newsletter to clarify payment procedures to all state agencies. The article instructs them to modify contracts to reflect increases in the invoiced amount rather than just adding a non-referencing line to the electronic invoice.

There are certain situations where adding a non-referencing line is acceptable. When paying against a master agreement or catalog master agreement, it is possible to add a line to cover an item that is authorized under the contractual agreement with the vendor, but that has not been added into the electronic catalog document in PD. For example, the office supply and building supply catalogs in PD are only partial lists of authorized items, and agencies cannot generate an invoice that references the master agreement without being able to add lines. The fact that catalogs are only partial lists is a function of the size of the catalog and the administrative burden of trying to keep it updated in a real-time manner. The agreement with Lowe's allows state agencies to purchase any item in the store at a discounted contract price. It is not practical to import that catalog into PD, nor is it possible to "punch out" from PD into the Lowe's online catalog.

Agencies have been specifically reminded about FAP 111-45-00 and FAP 111-11-00 in the MARS and Beyond *newsletter for MARS users in four issues during the past year alone on February 28, 2003, April 25, 2003, July 10, 2003, and January 16, 2004.*

MARS training provided by the cabinet covers these issues in the Procurement 101, General Procurement, Contracting, and PD Payment Processing classes. Procurement personnel are required to attend at least one procurement related training by 200 KAR 5:302, if the agency has a small purchase delegation above the minimum level established in KRS 45A.100.

SUMMARY SCHEDULE OF PRIOR AUDIT FINDINGS
FOR THE YEAR ENDED JUNE 30, 2003

Fiscal Year	Finding Number	Finding	CFDA Number	Questioned Costs	Comments
Reportable Conditions					
(1) Audit findings that have been fully corrected:					
FY 02	02-FAC-1	The Finance And Administration Cabinet Should Closely Monitor The Progress Of The Disparity Study Relating To Set-Aside Laws	N/A	0	Resolved during FY 03.
FY 02	02-FAC-5	The Finance And Administration Cabinet Should Work With American Management Systems To Strengthen Logical Security Measures Over The MARS And MRDB Database	N/A	0	Resolved during FY 03.
FY 02	02-FAC-6	The Finance And Administration Cabinet Should Work With The Governor's Office For Technology To Ensure The Security Log Report Is Generated, Recoverable, And Effectively Monitored	N/A	0	Resolved during FY 03.
FY 02	02-FAC-8	The Finance And Administration Cabinet Should Strengthen The Security Of Administrator Accounts	N/A	0	Resolved during FY 03.
FY 02	02-FAC-9	The Finance And Administration Cabinet Should Ensure That All Open Ports On Agency Machines Have A Business-Related Purpose	N/A	0	Due to improvements, this finding is downgraded to an other matter for FY 03. This finding is no longer required to be reported under *Government Auditing Standards*.
FY 01	01-FAC-6	The Office of Technical Services Should Improve Security Of The Servers Within The Local Area Networks For Finance and Administration Cabinet	N/A	0	Resolved during FY 03.
FY 01	01-FAC-7	The Finance And Administration Cabinet Should Implement Policies And Procedures To Ensure Compliance With Applicable Small Or Small Minority Business Set-Aside Laws	N/A	0	Resolved during FY 03.
FY 99	99-FAC-13	The Finance And Administration Cabinet Should Implement Policies And Procedures Relating To Small Or Small Minority Business Set-Aside Laws	N/A	0	Resolved during FY 03.

SUMMARY SCHEDULE OF PRIOR AUDIT FINDINGS
FOR THE YEAR ENDED JUNE 30, 2003

Fiscal Year	Finding Number	Finding	CFDA Number	Questioned Costs	Comments
Reportable Conditions (Continued)					
(2) Audit findings not corrected or partially corrected:					
FY 02	02-FAC-2	The Finance And Administration Cabinet Should Ensure Consistent Classification And Categorization Of Investments In The Cash And Investment Note.	N/A	0	The cash and investment note preparation process has improved, but improvements are still needed in the classification and categorization areas. See 03-FAC-1
FY 02	02-FAC-3	The Finance And Administration Cabinet Should Develop And Consistently Apply Formal Change Management Control Procedures For The Commonwealth's Cash And Investment Statistical Analysis System Programs	N/A	0	Although OFM has taken steps in attempt to improve a couple of the issues noted within this comment, weaknesses still reside. Further, the comment has been expanded and renamed to incorporate additional system development life cycle issues noted for FY 03. See 03-FAC-6
FY 02	02-FAC-4	The Office Of Financial Management Should Improve Segregation Of Duty Controls	N/A	0	Although OFM has taken action in an attempt to improve a couple of the issues noted within this comment, these actions are not deemed sufficient. Issues were again noted with OFM's segregation of duty controls for FY 03. See 03-FAC-7
FY 02	02-FAC-7	The Finance And Administration Cabinet Should Ensure All User Accounts On Its Agency Servers Are Necessary	N/A	0	Exceptions were noted during testing for FY 03 with some of the same machines and some new ones. See 03-FAC-3

SUMMARY SCHEDULE OF PRIOR AUDIT FINDINGS
FOR THE YEAR ENDED JUNE 30, 2003

Fiscal Year	Finding Number	Finding	CFDA Number	Questioned Costs	Comments
Reportable Conditions (Continued)					
(2) Audit findings not corrected or partially corrected:					
FY 01	01-FAC-2	The Finance And Administration Cabinet Should Improve Controls Over Preparation Of The Cash And Investment Note	N/A	0	The cash and investment note preparation process has improved, but improvements are still needed in the classification and categorization areas. See 03-FAC-1
FY 01	01-FAC-3	The Office Of Financial Management Should Improve Control Procedures Over Modifications To System Programs	N/A	0	See 03-FAC-6
FY 00	00-FAC-6	The Office Of Financial Management Should Improve Control Procedures Over Modifications To System Programs	N/A	0	See 03-FAC-6
(3) Corrective action taken is significantly different from corrective action previously reported:					
There were no findings to report for this section.					
(4) Audit finding is no longer valid or does not warrant further action:					
There were no findings to report for this section.					
Material Weaknesses					
1) Audit findings that have been fully corrected:					
There were no findings to report in this section.					
(2) Audit findings not corrected or partially corrected:					
There were no findings to report in this section.					
(3) Corrective action taken is significantly different from corrective action previously reported:					
There were no findings to report in this section.					
(4) Audit finding is no longer valid or does not warrant further action:					
There were no findings to report in this section.					

SUMMARY SCHEDULE OF PRIOR AUDIT FINDINGS
FOR THE YEAR ENDED JUNE 30, 2003

Fiscal Year	Finding Number	Finding	CFDA Number	Questioned Costs	Comments
Other Matters					
(1) Audit findings that have been fully corrected:					
FY 02	02-FAC-10	The Finance And Administration Cabinet Should Improve Investment Related Closing Package Forms And Instructions	N/A	0	Resolved during FY 03.
FY 02	02-FAC-11	The Office Of Financial Management Should Ensure Adequate And Consistent Reconciliations	N/A	0	Resolved during FY 03.
FY 02	02-FAC-12	The Office Of Financial Management Should Ensure Trading Limits Are Monitored	N/A	0	Resolved during FY 03.
FY 02	02-FAC-13	The Office Of Financial Management Should Ensure Adequate Segregation Of Duties	N/A	0	Resolved during FY 03.
FY 02	02-FAC-14	The Finance And Administration Cabinet Should Continue To Strengthen The Procedures For Recording Contingent Liabilities	N/A	0	Resolved during FY 03.
FY 02	02-FAC-15	The Finance And Administration Cabinet Should Closely Examine The Closing Packages Prepared By The Agencies For Accurate Completion	N/A	0	Resolved during FY 03.
FY 02	02-FAC-24	The Finance and Administration Cabinet Should Ensure The Agreement Between The United States Department Of The Treasury And The Commonwealth Is In Compliance With 31 CFR Part 205– Cash Management Improvement Act	N/A	0	Significant improvements were made concerning exceptions noted in prior FY. These improvements resulted in comment being downgraded to a verbal for FY 03.
FY 01	01-FAC-8	The Office Of Financial Management Should Improve MARS Reconciliation Procedures	N/A	0	Resolved during FY 03.
FY 01	01-FAC-10	The Finance and Administration Cabinet Should Ensure Agencies Follow The Closing Package Instructions Relating to Contingencies	N/A	0	Resolved during FY 03.

SUMMARY SCHEDULE OF PRIOR AUDIT FINDINGS
FOR THE YEAR ENDED JUNE 30, 2003

Fiscal Year	Finding Number	Finding	CFDA Number	Questioned Costs	Comments
Other Matters (Continued)					
(1) Audit findings that have been fully corrected: (Continued)					
FY 01	01-FAC-17	The Finance and Administration Cabinet Should Monitor Cash Management Improvement Act Eligible Projects To Ensure They Are Properly Recorded In MARS	N/A	0	Resolved during FY 03.
(2) Audit findings not corrected or partially corrected:					
FY 02	02-FAC-16	The Finance and Administration Cabinet should develop formal procedures for system assurance efforts concerning the Financial Analysis System.	N/A	0	Still pending resolution (is scheduled to be incorporated in design changes for FAS.V2) See 03-FAC-11
FY 02	02-FAC-17	The Finance and Administration Cabinet Should Work In Conjunction with the Governor's Office for Technology to Implement Logging And Audit Features Within Procurement Desktop	N/A	0	Resolution in progress, but not during the audit period under review. Currently pulling the daily logs in text and storing on DVDs. See 03-FAC-12
FY 02	02-FAC-18	The Finance and Administration Cabinet should consistently apply established program modification control procedures for the Financial Analysis System.	N/A	0	Still pending resolution (is scheduled to be incorporated in design changes for FAS.V2). See 03-FAC-13
FY 02	02-FAC-19	The Finance and Administration Cabinet should improve logical security measures over the Financial Analysis System.	N/A	0	Still pending resolution (is scheduled to be incorporated in design changes for FAS.V2) See 03-FAC-14
FY 02	02-FAC-20	The Finance and Administration Cabinet should develop and Implement formal written policies and procedures concerning security of the Financial Analysis System.	N/A	0	Still pending resolution (is scheduled to be incorporated in design changes for FAS.V2) See 03-FAC-15
FY 02	02-FAC-21	The Finance And Administration Cabinet Should Ensure That Security Information Leakage For Agency Devices Is Minimized	N/A	0	Improvements were made during the year, but issues still exist. Formal comment re-issued. See 03-FAC-16

SUMMARY SCHEDULE OF PRIOR AUDIT FINDINGS
FOR THE YEAR ENDED JUNE 30, 2003

Fiscal Year	Finding Number	Finding	CFDA Number	Questioned Costs	Comments
Other Matters (Continued)					
(2) Audit findings not corrected or partially corrected: (Continued)					
FY 02	02-FAC-22	The Finance And Administration Cabinet Should Change System Defaults To Guard Against Unauthorized System Access	N/A	0	Improvements were made during the fiscal year, but issues still exist. Formal comment re-issued. See 03-FAC-17
FY 02	02-FAC-23	The Finance And Administration Cabinet Should Strengthen Its Account Password Policy And Implement The Policy On All Domain Servers	N/A	0	Improvements were made during the fiscal year, but issues still exist. Formal comment re-issued. See 03-FAC-18
FY 02	02-FAC-25	The Finance and Administration Cabinet Should Review All Eligible Cash Management Improvement Act (CMIA) Transactions Requiring Interest Calculations To Ensure That the Annual Report Is Complete and Accurate.	N/A	0	There were some minor repeat issues noted again with the accuracy of the CMIA Annual Report for FY 2003. See 03-FAC-19
FY 01	01-FAC-11	The Finance and Administration Cabinet should develop and Implement formal written policies and procedures concerning security of the Financial Analysis System	N/A	0	Still pending resolution. (scheduled to be incorporated in design changes for FAS.V2) See 03-FAC-15
FY 01	01-FAC-12	The Finance and Administration Cabinet should improve logical security measures over the Financial Analysis System	N/A	0	Still pending resolution (scheduled to be incorporated in design changes for FAS.V2) See 03-FAC-14
FY 01	01-FAC-13	The Finance and Administration Cabinet should consistently apply established program modification control procedures for the Financial Analysis System	N/A	0	Still pending resolution (scheduled to be incorporated in design changes for FAS.V2) See 03-FAC-13
FY 01	01-FAC-14	The Finance and Administration Cabinet should develop formal procedures for system assurance efforts concerning the Financial Analysis System	N/A	0	Still pending resolution (scheduled to be incorporated in design changes for FAS.V2) See 03-FAC-11

SUMMARY SCHEDULE OF PRIOR AUDIT FINDINGS
FOR THE YEAR ENDED JUNE 30, 2003

Fiscal Year	Finding Number	Finding	CFDA Number	Questioned Costs	Comments
Other Matters (Continued)					
(2) Audit findings not corrected or partially corrected: (Continued)					
FY 01	01-FAC-15	The Finance And Administration Cabinet Should Work In Conjunction With The GOT To Implement Logging And Audit Features Within Procurement Desktop	N/A	0	Resolution still in progress. See 03-FAC-12
FY 01	01-FAC-16	The Finance and Administration Cabinet Should Ensure The Treasury – State Agreement Is In Compliance With 31 CFR Part 205 – Cash Management Improvement Act	N/A	0	There were issues again noted with the TSA for FY 02. New issues were added for FY 02 due to the need to comply with the revised CFR. See 03-FAC-19
FY 00	00-FAC-7	The Finance And Administration Cabinet Should Work In Conjunction With The Governor's Office For Technology To Implement Logging And Audit Features Within Procurement Desktop	N/A	0	Resolution still in progress. See 03-FAC-12
(3) Corrective action taken is significantly different from corrective action previously reported:					
There were no findings to report in this section.					
(4) Audit finding is no longer valid or does not warrant further action:					
There were no findings to report in this section.					